Email Processing Method, Email Processing Apparatus And Recording Medium

Background of the Invention

Field of the Invention

[0001] The present invention relates to a method of processing an email when broadcasting the email carrying the same data to a plurality of email addresses of recipients by using, for example, a mailing list and a method of processing an email when receiving the email transmitted via broadcast transmission. The present invention also relates to an apparatus for implementing such methods, and a recording medium for recording a computer program to cause a computer to function as such apparatus.

Description of the Related Art

[0002] In recent times, various cryptographic techniques are studied to realize safe data communications in connection with a rapid growth of computer network. So far, a common key cryptosystem in which an encryption key is equal to a decryption key, and a public key cryptosystem in which an encryption key is different from a decryption key are widely used. Data Encryption Standards (DES) adopted by National Institute of Standards and Technology of the U.S.A. is a typical example of the common key cryptosystem and Rivest Shamir Adleman (RSA) is a typical example of the public key cryptosystem.

[0003] Another cryptosystem is also proposed, which utilizes ID (Identity)

information identifying individuals involved in communications such as post office addresses, names and email addresses of the individuals. In this cryptosystem, a common encryption key is generated between a sender and a receiver based on the ID information.

[0004] ID-NIKS (ID-based Non-Interactive Key Sharing Scheme) is studied as the cryptosystem which uses the ID information and does not require preliminary communications between a sender and a receiver prior to cryptographic communications. The ID-NIKS cryptosystem does not need to exchange a public key and a secret key between the sender and receiver. In addition, the ID-NIKS cryptosystem does not require a key list and services from a third party. With the ID-NIKS cryptosystem, therefore, safe communications can be ensured between arbitrary users. In particular, this cryptosystem is convenient for users since no preliminary communications are necessary. Accordingly, it is supposed to be a core of the cryptosystem in the future.

[0005] Figure 5 of the accompanying drawings illustrates the principle of the ID-NIKS system. Supposing existence of a reliable center, a shared key generating system is established having the center as its core. In Figure 5, the ID information of an entity A is designated by "h (IDA)". "h (•)" represents a hash function. The center calculates a secret key SAi for an arbitrary entity A based on a center public information {PCi}, a center secret information {SCi} and the ID information h(IDA) of the entity A as shown below and distributes the secret key SAi to the entity A.

$$SAi=Fi(\{SCi\}, \{PCi\}, h(IDA))$$

[0006] The entity A produces a common key KAB for encryption and decryption of data to be transmitted between the entity A and an arbitrary

entity B as shown below, by utilizing the secret key {SAi} of the entity A itself, the center public information {PCi} and ID information h(IDB) of the entity B:

$$KAB=f(\{SAi\}, \{PCi\}, h(IDB))$$

[0007] In the meantime, the entity B produces another common key KBA to be utilized between the entities A and B. If KAB is always equal to KBA, the common keys KAB and KBA can be utilized as the encryption key and the decryption key between the entities A and B.

[0008] Now, transmission and reception of an email utilizing the above described ID-NIKS system will be described. First, the sender and receiver of the email respectively acquire a secret key prepared based on their own email addresses (their own ID information) from a center. The sender then generates a common key based on a public key generated based on the receiver's email address (receiver's ID information) and the acquired secret key, encrypts data with the generated common key, and transmits the encrypted data to the receiver via email. On the other hand, the receiver generates a common key based on a public key generated based on the sender's email address (sender's ID information) and the secret key and decrypts the data in the received email with the common key.

[0009] Safe sending and receiving of the email can be easily realized by encrypting and decrypting data in the above described manner. The DES (Data Encryption Standard) can be utilized in the above described ID-NIKS cryptographic communications.

[0010] A mailing list is usually used when sending the same email to a plurality of recipients. Specifically, an email server which handles (administers, manages) the mailing list broadcasts the email to a plurality of

email addresses registered in the mailing list. A plurality of users can therefore receive the same email.

[0011] As described earlier, however, the sender needs to encrypt data utilizing its own secret key and the email address of each recipient in the ID-NIKS system. Thus, the sender has to refer to email addresses of a plurality of recipients when broadcasting the same email to these recipients. Thus, the mailing list cannot be efficiently used in the ID-NIKS system.

Summary of the Invention

[0012] An object of the present invention is to provide an email processing method that can realize easy transmission and reception of emails including encrypted data to and from a plurality of recipients.

[0013] Another object of the present invention is to provide a recording medium that records a computer program for causing a computer to function as an apparatus for implementing such email processing method.

[0014] According to a first aspect of the present invention, there is provided a method of sending an email to a mailing list in which at least one recipient is registered, comprising the steps of: creating a common key from a public key generated based on an email address of the mailing list and a secret key generated based on an email address of a sender of the email; and sending an email, which includes data encrypted with the common key, to the email address of the mailing list.

[0015] Therefore, it is not necessary to encrypt the email data on the basis of email addresses of recipients respectively when sending the same email to

these recipients. It is only needed to encrypt the email data on the basis of the email address of the mailing list and the email address of the sender. The encrypted email is sent to the mailing list and in turn to the recipients. Accordingly, the email including the encrypted data can be transmitted to the recipients in an easy manner.

[0016] The secret key may be prepared by a center and supplied via email.

[0017] According to a second aspect of the present invention, there is provided an email processing method suited for when receiving an email addressed to a mailing list in which at least one recipient is registered, the email processing method comprising the steps of: creating a common key from a secret key generated based on an email address of the mailing list and a public key generated based on an email address of a sender of the email; and decrypting encrypted data included in the email with the common key.

[0018] When the recipients registered in the mailing list receive and decrypt the email addressed to the mailing list, the recipients utilize the common key derived from the email address of the mailing list and the email address of the email sender. Thus, the decryption of the email data can be done easily.

[0019] According to a third aspect of the present invention, there is provided a computer-readable recording medium comprising: first program code means for causing a computer to create a common key from a public key generated based on an email address of a mailing list, in which at least one recipient is registered, and a secret key generated based on an email address of a sender of the email; and second program code means for causing the computer to send an email including data encrypted with the common key to the email address of the mailing list.

[0020] According to a fourth aspect of the present invention, there is provided a computer-readable recording medium suited for when receiving an email addressed to a mailing list in which at least one recipient is registered, the email including encrypted data, the computer-readable recording medium comprising: first program code means for causing a computer to create a common key from a secret key generated based on an email address of the mailing list and a public key generated based on an email address of a sender of the email; and second program code means for causing the computer to decrypt encrypted data included in the email with the common key.

[0021] According to a fifth aspect of the present invention, there is provided an apparatus for sending an email to a mailing list in which at least one recipient is registered, the email including encrypted data, the apparatus comprising: means for creating a common key from a public key generated based on an email address of the mailing list and a secret key generated based on a predetermined email address; and means for sending the email including data encrypted with the common key, to the mailing list.

[0022] The apparatus may further include a recording medium for storing the secret key generated based on the predetermined email address.

[0023] According to a sixth aspect of the present invention, there is provided an apparatus for receiving an email addressed to a mailing list in which at least one recipient is registered, comprising: means for creating a common key from a public key generated based on an email address of a sender of the email and a secret key generated based on an email address of the mailing list; and means for decrypting encrypted data included in the email by utilizing the common key.

[0024] The apparatus may further include a recording medium for storing the secret key generated based on the email address of the mailing list.

Brief Description of the Drawings

[0025] Figure 1 is a block diagram showing an example of a mailing service system constituted by a plurality of personal computers (i.e., apparatus for carrying out the email processing method of the present invention) and a computer network connecting these personal computers.

[0026] Figure 2 is a block diagram showing a structure of one of the personal computers illustrated in Figure 1.

[0027] Figure 3 is a flowchart showing the procedure of the personal computer shown in Figure 1 when sending an email to a mailing list.

[0028] Figure 4 is a flowchart showing the procedure of other personal computers when receiving the email addressed to the mailing list.

[0029] Figure 5 schematically illustrates the principle of the ID-NIKS system.

Detailed Description of the Invention

[0030] An embodiment of the present invention will be described in detail in reference to the accompanying drawings.

[0031] Referring to Figure 1, illustrated is a block diagram of personal

computers PC1, PC2, ... , PCn (n: natural number) that function as apparatus for implementing an email processing method of the present invention, and a computer network connected to the personal computers PC1, PC2, ..., PCn.

[0032] In Figure 1, NTW designates the Internet that serves as the computer network. A number of Internet service providers PR1, PR2, ... , PRn (n: natural number) are connected to the Internet NTW.

[0033] The Internet service providers PR1, PR2, ..., PRn have servers SV1, SV2, ..., SVn (n: natural number) respectively that function as email servers for sending and receiving emails to and from their clients (i.e., subscribers). SMTP (Simple Mail Transfer Protocol) or POP3 (Post Office Protocol 3) is utilized as an email protocol in this embodiment.

[0034] The personal computers PC1, PC2, ..., PCn (i.e., clients) are connected to the servers SV1, SV2, ..., SVn of the providers PR1, PR2, ..., PRn via routers RT1, RT2, ..., RTn (n: natural number) and analogue lines L.

[0035] A center C issues first secret keys PRK1-1, PRK1-2, ..., PRK1-n to respective users. The first secret keys PRK1-1, PRK1-2, ..., PRK1-n are prepared on the basis of email addresses of the respective users and sent to the respective personal computers PC1, PC2, ..., PCn secretly by means of email or the like.

[0036] The center C also issues a second secret key PRK2 to a mailing list. The second secret key PRK2 is prepared on the basis of the email address of the mailing list and sent to an email server MS that handles the mailing list by means of email or the like. This email server is referred to as "ML server" hereinafter.

[0037] The ML server MS secretly sends an email including the second secret key PRK2 received from the center C to the email addresses registered in the mailing list. Thus, each of the personal computers PC1, PC2, ..., PCn can receive the second secret key PRK2.

[0038] It should be noted that a flexible disk that stores a first secret key PRK1 may be delivered to each personal computer from the center C by post instead of sending the first secret key by email. Likewise, a flexible disk that stores the second secret key PRK2 may be delivered to each personal computer from the ML server MS by post, and a flexible disk that stores the second secret key PRK2 may be delivered to the ML server MS from the center C by post.

[0039] A database server DS is connected to the network NTW. The database server DS has a recording medium DB that has recorded a program to operate an email sending apparatus of the present invention. The personal computer PC1 is the email sending apparatus if the personal computer PC1 transmits the email to other personal computers PC2, ..., PCn.

[0040] Referring to Figure 2, illustrated is a block diagram of the personal computer PC1 that functions as an apparatus for implementing the email processing method of the present invention. It should be noted that the structures of the personal computers PC2, PC3, ..., PCn are the same as that of the personal computer PC1, so that the description of the personal computers PC2, PC3, ..., PCn will be omitted.

[0041] In Figure 2, the reference numeral 1 designates a control unit that includes a CPU, a cash memory, etc. The control unit 1 controls each hardware element connected thereto via a bus 8. The control unit 1 also executes various computer programs stored on a hard disk 4 (will be described).

[0042] A RAM 2 includes an SRAM and/or a DRAM, and stores temporary data generated in the controller 1.

[0043] An external memory device 3 includes a CD-ROM drive and/or a flexible disk drive, and reads programs from a portable recording medium 10 such as a CD-ROM and/or a flexible disk. The programs for the email sending method and/or the email processing method of the present invention are recorded on the portable recording medium 10.

[0044] A hard disk 4 is a readable and writable magnetic disk, and stores programs for the email apparatus of the present invention, which are read by the external memory device 3, and various computer programs necessary for the operation of the personal computer PC1.

[0045] The hard disk 4 also stores the first secret key PRK1-1 and the second secret key PRK2 supplied from the center C.

[0046] It should be noted that Figure 2 shows the structure of the personal computer PC1 so that the hard disk 4 stores the first secret keys PRK1-1. In case of the personal computer PC2, however, the hard disk 4 stores the first secret key PRK1-2, and in case of the personal computer PCn the hard disk 4 stores the first secret key PRK1-n.

[0047] The first secret key PRK1-1 is utilized when sending an email, and the second secret key PRK2 is utilized when receiving an email addressed to the mailing list (will be described in detail). Therefore, the second secret key PRK2 is not necessarily stored in the hard disk 4 if the personal computer PC1 only sends an email and does not receive any emails directed to the mailing list (i.e., via the ML server).

[0048] A modem 5 is a communication interface for data communications via the Internet NTW, and connects and disconnects the personal computer PC1 to and from the analogue circuit L. It should be noted that the personal computer PC1 can be connected to a digital circuit or network of a baseband transmission system by utilizing a DSU (Digital Service Unit) instead of the modem 5.

[0049] A display unit 6 is a CRT display and/or a liquid crystal display (LCD), and displays an operating condition of the personal computer PC1 and various input and output data. An operation unit 7 is a data entry device such as the keyboard necessary for operating the personal computer PC1.

[0050] It should be noted that the program for the email processing method of the present invention can be read from other than the portable recording medium 10. For example, by connecting the personal computer PC1 to the database server DS via the Internet NTW, the program can be downloaded from the recording medium DB provided in the database server DS. The downloaded program is then is stored in the hard disk 4. The personal computer PC1 can therefore implement a process (will be described) when the control unit 1 loads the program into RAM 2 from the hard disk 4.

[0051] Next, the operation of the personal computers PC1, PC2, ..., PCn will be described.

[0052] Figure 3 is a flowchart showing the procedure of the control unit 1 when the personal computer PC1 sends an email to the mailing list. It should be assumed that the personal computer PC1 has finished the logging in operation by sending the user ID, the password, etc. to the provider PR1 which the personal computer PC1 has subscribed for.

[0053] A user who subscribes for the mailing list service handled (controlled, managed) by the ML server MS operates the operation unit 7 to input the email address of the mailing list. The mail address of the mailing list is a destination of the email. The user also enters data to be transmitted via email. The user then instructs the personal computer PC1 to send the email.

[0054] The control unit 1 provided in the personal computer PC1 reads the public key specified based on the email address of the mailing list and the first secret key PRK1-1 stored in the hard disk 4 when the personal computer PC1 accepts the email transmission instruction from the user (Step S11).

[0055] Next, the control unit 1 creates a common key from the public key and the first secret key PRK1-1 that are read in Step S11 (Step S12). The input data is then is encrypted by the DES scheme or the like with the common key (Step S13).

[0056] The control unit 1 sets the email address of the mailing list, which is input by the user, to the email destination and prepares the email by utilizing the encrypted data (Step S14). The prepared email is sent to the ML server MS (Step S15).

[0057] The email sent from the personal computer PC1 is received by the ML server MS via the server SV1. The ML server MS broadcasts the email received from the personal computer PC1 to the email addresses registered in the mailing list.

[0058] Figure 4 is a flowchart showing the operation of the control unit 1 of each of the personal computers PC2, ..., PCn when each of the personal computers PC2, ..., PCn receives the email, which is addressed to the mailing list. It should be assumed that the personal computers PC2, ..., PCn have

already logged in by sending the user IDs, the passwords, etc. to the providers PR2, ..., PRn which the personal computers PC2, ..., PCn have subscribed for respectively.

[0059] Each of users of the personal computers PC2, ..., PCn who subscribes for the mailing list service handled by the ML server MS instructs his or her own personal computer PC2, ..., PCn to receive the email. The control unit 1 of each personal computer PC2, ..., PCn receives and reads the email addressed to the mailing list, which is sent from the ML server MS, from the associated server SV2, ..., SVn when the control unit 1 accepts the email reception instruction from the user (Step S21).

[0060] Next, the control unit 1 reads the second secret key PRK2 from the hard disk 4 (Step S22). The control unit 1 creates a common key from the second secret key PRK2 and a public key generated based on the email address of the sender of the email that is read in Step S21 (Step S23). The control unit 1 then decrypts the data of the received email with the common key (Step S24).

[0061] Therefore, each of the users of the personal computers PC2, ..., PCn can see and read the content of the encrypted email addressed to the mailing list.

[0062] The sending and receiving of the email is implemented by using the mailing list in the illustrated embodiment, but the present invention can be applied to a system which does not rely upon the mailing list, as long as the same email can be broadcasted to a plurality of recipients when a single email address is designated as the email destination.

[0063] This application claims priority of Japanese Patent Application No. 2001-17516 filed on January 25, 2001, and the entire disclosure thereof is

incorporated herein by reference.